Администрирование сетевых подсистем

Лабораторная работа №7

Авдадаев Джамал Геланиевич

28 ноября 2025

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Цель лабораторной работы

Получение практических навыков настройки межсетевого экрана firewalld, создания пользовательских служб, перенаправления портов и включения Masquerading.

Ход выполнения

Создание пользовательской службы firewalld

```
[root@server.dgavdadaev.net server]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
[root@server.dgavdadaev.net server]# cd /etc/firewalld/services/
[root@server.dgavdadaev.net services]# cat ssh-custom.xml
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>SSH</short>
  <description>Secure Shell (SSH) is a protocol for logging into and executing commands on remote machines. It provides secure encrypted
communications. If you plan on accessing your machine remotely via SSH over a firewalled interface, enable this option. You need the open
ssh-server package installed for this option to be useful.</description>
  <port protocol="tcp" port="22"/>
</service>
[root@server.dgavdadaev.net services]#
```

Рис. 1: Создание файла ssh-custom.xml

Изменение порта и описания службы

Рис. 2: Редактирование ssh-custom.xml

Проверка списка служб и активация

```
[root@server.dgavdadaev.net services]# firewall-cmd --get-services
0-AD RH-Satellite-6 RH-Satellite-6-capsule afp alvr amanda-client amanda-k5-client amqp amqps anno-1602 anno-1800 apcupsd aseqnet audit a
usweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testn
et-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent civilization-iv civilization-v cockpit collectd condor-collector
 cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-quic dns-over-tls docker-registry docker-swarm
dropbox-lansync elasticsearch etcd-client etcd-server factorio finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-
replication freeipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-availability http http3 https ident imap ima
ps iperf2 iperf3 ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshe
ll kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodep
ort-services kube-scheduler kube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls ligh
tning-network llmnr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache minecraft minidlna mndp mongodb mosh mountd mpd mqt
t mqtt-tls ms-wbt mssql murmur mysql nbd nebula need-for-speed-most-wanted netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut o
pentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privox
y prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius radsec rdp redis redis-sent
inel rootd rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane settlers-history-collection sip sips slimevr slp
 smtp smtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squid ssdp ssh ssh-custom statsrv steam-lan
-transfer steam-streaming stellaris stronghold-crusader stun stuns submission supertuxkart svdrp svn syncthing syncthing-gui syncthing-re
lay synergy syscomlan syslog syslog-tls telnet tentacle terraria tftp tile38 tinc tor-socks transmission-client turn turns upnp-client vd
sm vnc-server vrrp warpinator wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-host ws-discovery-tcp ws-disco
very-udp wsdd wsdd-http wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-java-gateway zabbix-server za
bbix-trapper zabbix-web-service zero-k zerotier
[root@server.dgavdadaev.net services]#
[root@server.dgavdadaev.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
[root@server.dgavdadaev.net services]# firewall-cmd --add-service=ssh-custom
success
[root@server.dgavdadaev.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh ssh-custom
[root@server.dgavdadaev.net services]# firewall-cmd --add-service=ssh-custom --permanent
success
[root@server.dgavdadaev.net services]# firewall-cmd --reload
success
[root@server.dgavdadaev.net services]#
```

Рис. 3: Активация службы

Настройка перенаправления порта

```
[root@server.dgavdadaev.net services]#
[root@server.dgavdadaev.net services]#
[root@server.dgavdadaev.net services]# firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22
success
[root@server.dgavdadaev.net services]#
```

Рис. 4: Настройка перенаправления 2022→22

Подключение клиента по новому порту

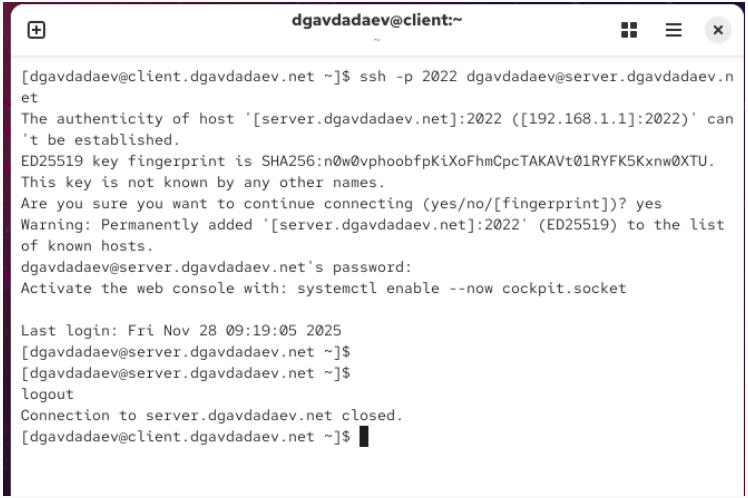

Рис. 5: SSH через порт 2022

Включение IPv4 forwarding и masquerading

```
net.ipv4.ip_forward_use_pmtu = 0
net.ipv6.conf.all.forwarding = 0
net.ipv6.conf.all.mc_forwarding = 0
net.ipv6.conf.default.forwarding = 0
net.ipv6.conf.default.mc_forwarding = 0
net.ipv6.conf.eth0.forwarding = 0
net.ipv6.conf.eth0.mc_forwarding = 0
net.ipv6.conf.eth1.forwarding = 0
net.ipv6.conf.eth1.mc_forwarding = 0
net.ipv6.conf.lo.forwarding = 0
net.ipv6.conf.lo.mc_forwarding = 0
[root@server.dgavdadaev.net services]#
[root@server.dgavdadaev.net services]# echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf
[root@server.dgavdadaev.net services]# sysctl -p /etc/sysctl.d/90-forward.conf
net.ipv4.ip_forward = 1
[root@server.dgavdadaev.net services]# firewall-cmd --zone=public --add-masquerade --permanent
success
[root@server.dgavdadaev.net services]# firewall-cmd --reload
success
[root@server.dgavdadaev.net services]#
```

Рис. 6: Включение forwarding и masquerading

Подготовка конфигурации для Vagrant provision

```
[root@server.dgavdadaev.net services]#
[root@server.dgavdadaev.net services]# cd /vagrant/provision/server/
[root@server.dgavdadaev.net server]# mkdir -p /vagrant/provision/server/firewall/etc/firewalld/services
[root@server.dgavdadaev.net server]# mkdir -p /vagrant/provision/server/firewall/etc/sysctl.d
[root@server.dgavdadaev.net server]# cp -R /etc/firewalld/services/ssh-custom.xml /vagrant/provision/server/firewall/etc/firewalld/servic
es
[root@server.dgavdadaev.net server]# cp -R /etc/sysctl.d/90-forward.conf /vagrant/provision/server/firewall/etc/sysctl.d
[root@server.dgavdadaev.net server]# touch firewall.sh
[root@server.dgavdadaev.net server]#
```

Рис. 7: Копирование конфигураций в provision

Скрипт автоматизации firewall

```
#!/bin/bash
echo "Provisioning script $0"
echo "Copy configuration files"
cp -R /vagrant/provision/server/firewall/etc/* /etc
echo "Configure masquerading"
firewall-cmd --add-service=ssh-custom --permanent
firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22 --permanent
firewall-cmd --zone=public --add-masquerade --permanent
firewall-cmd --reload
restorecon -vR /etc

```

Рис. 8: firewall.sh

Выводы

Итог лабораторной работы

Была создана пользовательская служба firewalld с новым портом, выполнено перенаправление трафика, включено пересылание IPv4-пакетов и настроен маскарадинг.

SSH-подключение по новому порту проверено с клиентской машины.

Конфигурации перенесены в директорию Vagrant provisioning, создан автоматический скрипт firewall.sh.

Итоговая среда успешно функционирует и готова для повторного развёртывания.